Guia de Boas Práticas de Segurança para E-Commerce

(Desenvolvedor do Software)

Versão 10.04.2012

abecs - associação brasileira das empresas de cartão de crédito e serviços
www.abecs.org.br Segurança e Prevenção a Fraude

Realizar negócios através da Internet é uma alternativa de alto valor estratégico para os empresários que optaram por investir neste segmento. Os limites geográficos são removidos e os custos operacionais são consideravelmente menores em comparação com os negócios baseados em lojas físicas.

Este é um mercado que tem se desenvolvido em ritmo elevado e a tendência é que este curso de elevação seja mantido, pois, com o crescimento da economia e as ações do governo federal no sentido de democratizar o acesso a tecnologia se espera um aumento expressivo no volume de novos consumidores na Internet, sobretudo aqueles que recentemente alcançaram a classe média.

Um cenário tão favorável para novos negócios e com alta circulação de dinheiro desperta o interesse de criminosos que buscam tornar seus golpes cada vez mais sofisticados à medida que a tecnologia evolui.

Se proteger desta modalidade de crime é uma tarefa que exige o esforço de todos. No entanto, as pequenas e médias empresas são as que se tornam mais vulneráveis ao crime eletrônico, devido ao fato de que, para manterem custos competitivos, geralmente não possuem profissionais com foco em desenvolver e manter ambientes e sistemas seguros.

Acreditamos que a chave para a proteção do mercado, sobretudo o do comércio eletrônico, reside no compartilhamento do conhecimento. Desta forma, este guia possui o objetivo orientar empresários, profissionais de infraestrutura tecnológica e desenvolvedores de sistemas ligados ao Comércio Eletrônico no sentido de proteger suas aplicações web reduzindo riscos de ataques, comprometimento de informações e fraudes. Serão descritas aqui as formas mais comuns de ataques na Internet e formas de proteção com uma linguagem acessível, de acordo com a atividade desempenhada por cada profissional.

Boa leitura.

1. Vulnerabilidades no desenvolvimento de software

Atualmente boa parte dos ataques contra aplicações web ocorrem devido a falhas no desenvolvimento de software que deixam brechas para a entrada de um invasor. Estas vulnerabilidades podem ter origem em todas as etapas do processo de desenvolvimento de software, desde ao design até a administração do sistema.

1.1. Falhas no Design

São os problemas gerados no planejamento da Aplicação Web, quando estas são desenhadas e desenvolvidas sem que haja uma preocupação adequada com o nível de segurança. Controlar acessos aos aplicativos somente por meio de quais menus cada usuário poderá ver ou as simplificações no acesso a base de dados são exemplos comuns de falhas deste tipo.

1.2. Falhas na Arquitetura

São as vulnerabilidades associadas à segmentação de redes, implementação de ativos de TI e informações que possam comprometer o ambiente analisado. Manter o banco de dados que suporta um web site na DMZ possibilitando o acesso remoto externo sem autenticação, é um exemplo comum. É comum ainda a presença de protocolos de comunicação com falhas que podem ser exploradas para burlar o processo de criptografia estabelecido.

1.3. Falhas no Código

São as falhas relacionadas à maneira em que as empresas constroem suas aplicações corporativas, frameworks e demais componentes do software. É a camada onde são identificadas as falhas mais comuns..

1.4. Falhas na Administração

Problemas gerados não pela Aplicação Web em si, mas sim pela forma como ela é administrada onde os conceitos de proteção não são aplicados como esperado. Exemplos comuns ocorrem na remoção de determinados controles previamente planejados, como a mudança de senhas fortes para controles mais fracos a pedido de uma área, para atender a uma necessidade de negócio que não tenha tido o seu nível de risco devidamente avaliado.

2. Proteção do software

Proteger aplicações web requer a implementação de controles de segurança em todo ciclo de vida do desenvolvimento de software. Abaixo as principais regras para melhorar o nível de segurança do software desenvolvido em sua empresa, contemple-as em sua metodologia de desenvolvimento de software.

Obs.: As regras definidas neste documento, embora garantam uma elevação considerável do nível de segurança em aplicações web, não encerram completamente a questão. **É importante que os desenvolvedores se mantenham atualizados com relação às novas vulnerabilidades e contramedidas a serem aplicadas em seu software.** A participação em fóruns como o OWASP[1], o estudo e a constante atualização em sites especializados são altamente recomendáveis.

2.1. Mantenha os desenvolvedores sempre atualizados com relação às novas vulnerabilidades e formas de proteção.

2.2. Nunca armazene usuários e senhas ou chaves criptográficas de sua aplicação no código fonte. Procure utilizar serviços de autenticação como o RADIUS ou criptografar estes dados.

2.3. Nunca permita que a sua aplicação receba dados de usuários e senhas em texto claro. Utilize sempre do protocolo SSL.

2.4. Estabeleça uma política de senhas para a sua aplicação que de acordo com as regras abaixo:

2.4.1. Comprimento mínimo de 8 caracteres;

2.4.2. Período de expiração de no mínimo 45 dias;

2.4.3. Obrigatoriedade de que a senha seja composta de caracteres numéricos e alfanuméricos;

2.4.4. Obrigatoriedade de o usuário, ao compor uma nova senha não utilize nenhuma das quatro senhas anteriores.

2.5. Não envie a senha por e-mail nos casos em que o usuário executa a função “esqueci minha senha”. Procure usar mecanismos como o de pergunta secreta, etc.

2.6. Não armazene cookies com o usuário e a senha, mesmo que criptografados, na estação do usuário.

1 O OWASP é um fórum internacional, aberto e sem fins lucrativos que reúne profissionais com o objetivo de documentar vulnerabilidades em aplicações web e suas formas de prevenção. Anualmente o OWASP divulga o Top 10 com as dez falhas mais exploradas globalmente. Mais informações em https://www.owasp.org/index.php/Main_Page

2.7. Se certifique que a função de “logout” de sua aplicação realmente encerra completamente a sessão.

2.8. Insira um botão de “logout” em cada uma das páginas.

2.9. Conceda ao usuário de serviço de sua aplicação somente os acessos mínimos para o seu funcionamento. Nunca o defina como root, administrador ou sa.

2.10. Desenvolva permissões de acesso de acordo com cada funcionalidade da aplicação e não por menus.

2.11. Implemente mecanismos validação da entrada de dados em sua aplicação impedindo que seja possível a inserção de dados de um tamanho ou tipo (numérico, alfanumérico, data/hora, etc.) que contrarie a regra de negócio estabelecida no sistema.[2]

2.12. Implemente mecanismos de geração de logs, sobretudo para as transações críticas.

2.13. Armazene os logs em arquivos ou bancos de dados com acesso disponível somente às equipes de infraestrutura.

2.14. Realize o tratamento de erros impedindo a ocorrência de mensagens de erro com origem no sistema de banco de dados ou no webserver.

2.15. Impeça que sua aplicação armazene o número do cartão completo. Somente o armazene de maneira parcial mantendo somente as quatro últimas posições (ex.: ********** 1234) ou em modo criptografado.

2.16. Se o nome do portador do cartão e a data de vencimento forem armazenados em conjunto com o numero do cartão estes deverão estar em modo criptografado.

2.17. Não armazene em hipótese alguma as informações do código de segurança.

2.18. Estabeleça uma política de descarte dos dados do cartão em no mínimo um ano.

2.19. Não armazene informações de produção nos ambientes de desenvolvimento e homologação.

2.20. Remova todas as informações e contas de usuário de testes ao migrar o sistema para o ambiente de produção.

2.21. Estabeleça procedimentos, com periodicidade ao mínimo anual, de teste de intrusão com foco na tentativa de exploração de vulnerabilidades em aplicações web.

2 Mais informações sobre como implementar os mecanismos de validação de dados em http://ufpr.dl.sourceforge.net/project/owasp/Guide/2.0.1/OWASPGuide2.0.1.pdf

2.22. Elimine as vulnerabilidades reportadas em, pelo menos um mês após a detecção.

1. Glossário

Antivírus – Programa com o objetivo de proteger o computador contra vírus.

Autenticação – Mecanismo de validação da identidade de um usuário no momento que este acessa um sistema.

Certificado digital – Mecanismo utilizado para estabelecer a comunicação entre computadores com segurança.

Código fonte – Instruções em uma determinada linguagem de programação que, em conjunto compõem um software.

Cookie – Mecanismo utilizado em aplicações web que armazena dados de acesso na estação do usuário possibilitando a persistência de uma sessão de acesso. Um exemplo, são os cookies que armazenam informações de conexão para que o usuário não tenha que digitá-las novamente em outras visitas ao site.

Criptografia – Conjunto de técnicas com o objetivo de proteger uma informação de modo que esta só possa ser compreendida pelo remetente e pelo destinatário. O que protege a mensagem criptografada é a chave criptográfica, esta seria um segredo trocado previamente entre o remetente e o destinatário por meio do qual as mensagens serão criptografadas.

Criptografia Assimétrica – Forma de criptografia na qual o remetente e o destinatário não possuem a chave inteira mas sim partes dela que quando combinadas permitem decriptar a informação.

Criptografia Simétrica – Forma de criptografia na qual tanto o remetente quanto o destinatário compartilham a mesma chave para criptografar e decriptar informações.

DMZ - Abreviação de *demilitarized zone* (em português, zona desmilitarizada). Termo com origem no vocabulário militar que foi adaptado na informática para definir uma área de rede entre a rede interna e a internet.

Dupla custódia - Processo no qual uma chave de criptografia ou senha é elaborada por duas pessoas. Cada uma delas insere no sistema uma parte da chave. As duas partes são escritas e lacradas em envelopes separados e armazenados em cofre.

Firewalls – Dispositivos com a função de segregar redes realizando a proteção de um determinado perímetro. Nos firewalls os administradores determinam quais conexões são permitidas de uma rede para a outra.

Framework – Conjunto de conceitos técnicos que orienta o desenvolvimento de software.

FTP – File Transfer Protocol. Protocolo utilizado em redes de computadores para a transferência de arquivos.

HTTPS - HyperText Transfer Protocol Secure. Protocolo de acesso a páginas na internet com criptografia.

IDS – Intrusion Detection System – Mecanismo utilizado para analisar o comportamento do tráfego em uma rede e, com base em uma biblioteca de comportamentos conhecidos detectar e alertar o administrador sobre uma possível invasão.

IPS – Intrusion Prevention System – Semelhante ao IDS, entretanto com a funcionalidade de executar uma ação (o bloqueio da comunicação, por exemplo) quando um possível ataque é detectado.

Logon – Ato de acessar um sistema após o processo de autenticação (digitação do usuário e a senha, por exemplo).

Logout – Ato de encerrar o acesso a um sistema.

Logs – Também conhecidos como trilhas de auditoria. São arquivos ou bancos de dados com o registro de atividade de um determinado sistema ou dispositivo.

Memória não volátil – Memória na qual o conteúdo armazenado não é eliminado após o computador ser desligado. Por exemplo, discos rígidos, pendrives, CD-ROM, etc.

NAT - Network Address Translation – Técnica que consiste na conversão do endereço IP de origem em meio a uma conexão. Muito usado em situações nas quais computadores de uma rede interna precisam acessar endereços da Internet. Nestes casos, embora a conexão parta de um determinado endereço, este é alterado na saída para a Internet de modo que o endereço interno não é divulgado externamente.

Portas TCP/IP – Elemento utilizado em redes de computadores para separar a comunicação de dos protocolos. Exemplo: o protocolo FTP utiliza por padrão a porta 21.

Protocolos – Conjunto de regras que determinam formas de comunicação entre computadores.

PROXY-ARP – Mecanismo que possibilita a definição de somente um endereço IP para várias redes.

RADIUS - Remote Authentication Dial In User Service – Mecanismo com o objetivo de autenticar acessos a um determinado sistema. Mais informações em http://freeradius.org/

Root – Usuário administrador padrão de sistemas operacionais UNIX e Linux.

Roteadores – Equipamentos utilizados para estabelecer a comunicação entre duas ou mais redes de computadores.

SA – Usuário administrador padrão de sistemas de banco de dados SQL da Microsoft

Scan – Atividade de varredura presente em sistemas de antivírus ou ferramentas de análise de vulnerabilidades que realizam um scan em vários detalhes de um computador em busca de falhas.

SFTP – Protocolo FTP com uma camada de criptografia.

Software – Programa ou código executável para computador ou dispositivo semelhante.

SOURCE-Routing – Propriedade presente em alguns roteadores que possibilita ao usuário do computador de origem determinar uma rota de acesso remotamente. Seria como se este usuário tivesse a possibilidade de definir qual caminho seguiria em uma determinada conexão. Este é um mecanismo usado para ataques.

SSH – Protocolo que permite o estabelecimento de uma sessão remota com criptografia. Geralmente utilizado por administradores para gerenciar servidores e dispositivos de rede à distância.

SSL – Protocolo que estabelece criptografia em uma conexão a sites na internet. A presença da expressão HTTPS:\\ no endereço de um site geralmente é um indicativo de que a conexão está criptografada com SSL.

SSLv3 – Versão 3 do SSL.

Stateful inspection – Mecanismo presente em alguns firewalls no qual cada fragmento da conexão é inspecionado em busca de ataques.

Switches – Equipamentos utilizados para conectar computadores em uma rede.

TELNET - Protocolo que permite o estabelecimento de uma sessão remota. Geralmente utilizado por administradores para gerenciar servidores e dispositivos de rede à distância.

Teste de intrusão – Procedimento no qual um profissional aplica técnicas de ataque na rede ou sistemas de seu cliente com o intuito de reportar as vulnerabilidades do ambiente.

Tratamento de erros – Atividade do processo de desenvolvimento de sistemas que consiste em prever falhas na aplicação e definir mensagens de erro específicas para cada cenário de erro.

Usuários de serviço – Contas de acesso utilizadas por sistemas.

Vírus – Softwares com o objetivo de danificar computadores.

VPN – Virtual Private Networks – Meio de conexão remota criptografada na qual computadores podem estabelecer conexão entre si através da internet.

Webserver – Servidor com o objetivo hospedar páginas ou outros serviços disponíveis na internet.

WEP - Wired Equivalent Privacy – Mecanismo de autenticação em redes wireless obsoleto e com baixo nível de segurança

WPA - Wi-Fi Protected Access – Mecanismo de autenticação em redes wireless o qual substituiu o WEP, mas também é considerado pouco seguro.

WPA2 – Evolução do WPA, com maior nível de Segurança.